

FILED

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

UNITED STATES DISTRICT COURT
for the
Northern District of New York

Apr 04 - 2025

John M. Domurad, Clerk

In the Matter of the Seizure of
(Briefly describe the property to be seized)
The Domain Name: NFT-UNI.com

)
)
)
)
)

Case No. 1:25-SW-78 (PJE)

**APPLICATION FOR A WARRANT
TO SEIZE PROPERTY SUBJECT TO FORFEITURE**

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Eastern District of Virginia is subject to forfeiture to the United States of America under 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1).
(describe the property):

The Domain Name: NFT-UNI.com

The application is based on these facts:

Please see attached Affidavit.

☒ Continued on the attached sheet.

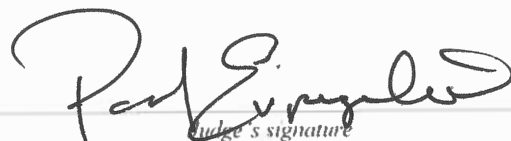

Applicant's signature

William Henry IV, Special Agent USSS

Printed name and title

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

Date: April 4, 2025


Judge's signature

City and state: Albany, New York

Hon. Paul J. Evangelista, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEIZURE OF:) Case No.: ~~1:25-mj-125-mj~~
) 1:25-SW-78 (PJE)
)
)
)
)
)
The Domain Name: NFT-UNI.com)

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, **William Henry IV**, being duly sworn, hereby declare as follows:

INTRODUCTION

1. I am a Special Agent with the United States Secret Service (“USSS or “Secret Service”), currently assigned to the Albany, NY Resident Office. I have graduated from the 400-hour Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. I have attended a 40-hour program at the National Computer Forensics Institute in Hoover, Alabama taught by computer specialists. I graduated the Special Agent Training Course taught by the USSS and completed an estimated 520 hours of training. I have a bachelor’s degree in criminal justice from Columbia College of Missouri and was previously a United States Army Paratrooper in the 82nd Airborne Division. My experience also consists of a prior Domain Seizure and I am familiar with the patterns and practices of individuals involved in committing wire fraud and money laundering by using cryptocurrency.

2. As set forth below, there is probable cause to believe that NFT-UNI.com (“**Target Domain**”), is property used, or intended to be used, to commit or facilitate violations of 18 U.S.C. § 1956(a)(1)(B)(i). Specifically, there is probable cause to believe that the **Target Domain** was involved in transactions designed to conceal the nature, location, source, ownership, and/or control of the proceeds of violations of 18 U.S.C. § 1343 (Wire Fraud), and are accordingly, subject to

seizure and forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1).

3. I make this affidavit for a warrant to seize the **Target Domain**, as described in Attachment A. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. Where statements of others are related in this affidavit, they are related in substance and in part.

4. The requested warrant is sought so that the government may prevent further use of the **Target Domain** to defraud additional victim and launder their funds.

5. The procedure by which the government will seize the **Target Domain** is more particularly described below and in Attachment A.

BACKGROUND ON DOMAIN NAMES

6. Based on my training and experience and information learned from others, I am aware of the following:

7. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

8. Domain Name: A domain name is a simple, easy-to-remember way for humans to

identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, “usdoj.gov” and “cnn.com” are domain names.

9. Domain Name System: The domain name system (“DNS”) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or “labels,” that are delimited by periods, such as “www.example.com.” The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the “top-level” domain. For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, the “example” second-level domain, and is the web server.

10. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol (“IP”) addresses.

11. Registry: For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. For example, the registry for the “.com” and “.net” top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

12. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. Registrars typically maintain customer and billing

information about the registrants who used their domain name registration services.

13. Whois: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0- 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

RELEVANT STATUTORY PROVISIONS

14. The United States seeks a dual-purpose seizure warrant allowing for the seizure of the **Target Domain** under both the criminal and civil forfeiture provisions of the United States Code.

A. Criminal Statutes

15. Concealment money laundering, as set forth in 18 U.S.C. § 1956(a)(1)(B)(i), makes it a crime to conduct or attempt to conduct a financial transaction involving the proceeds of specified unlawful activity knowing that the transaction is designed, in whole or in part, to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the specified unlawful activity.

16. Wire fraud offenses, as set forth in 18 U.S.C. § 1343, are designated as specified unlawful activities pursuant to 18 U.S.C. § 1956(c)(7) by 18 U.S.C. § 1961(1).

17. Title 18, United States Code, Section 1343, makes it a crime to knowingly execute, or attempt to execute, a scheme or artifice to (1) obtain money or property by means of false or fraudulent pretenses, representations, or promises; (2) that are material; (3) with the intent to

defraud; and (4) where the defendant used, or caused to be used, a wire communication to carry out or attempt to carry out an essential part of the scheme.

B. Forfeiture Authority

18. As described below, there is probable cause to believe that the **Target Domain** is property involved in offenses in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and is thereby subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and to criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

C. Civil Seizure Warrant Authority

19. The government may request the issuance of a civil seizure warrant for property involved in a violation of 18 U.S.C. § 1956 pursuant to 18 U.S.C. § 981(b)(1).

20. 18 U.S.C. § 981(b)(1) provides, as follows:

(b)(1) Except as provided in section 985, any property subject to forfeiture to the United States under subsection (a) may be seized by the Attorney General and, in the case of property involved in a violation investigated by the Secretary of the Treasury or the United States Postal Service, the property may also be seized by the Secretary of the Treasury or the Postal Service, respectively.

D. Criminal Seizure Warrant Authority

21. The government may request the issuance of a criminal seizure warrant for property involved in violation of 18 U.S.C. § 1956 pursuant to 21 U.S.C. § 853(f) by 18 U.S.C. § 982(b)(1).

22. 21 U.S.C. § 853(f) provides, as follows:

[t]he government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) of this section may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

23. 18 U.S.C. § 982(b)(1) provides, as follows:

(b)(1) The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

JURISDICTION & VENUE

24. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a “district court of the United States that has jurisdiction over the offense being investigated.” *See* 18 U.S.C. § 2711(3)(A)(i).

25. Venue is appropriately situated in this district pursuant to 28 U.S.C. §§ 1355(b)(1)(A) and 1395, because the acts or omissions giving rise to the forfeiture occurred in this district.

26. Pursuant to 18 U.S.C. § 981(b)(3), a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under 28 U.S.C. § 1355(b), any may be executed in any district in which the property is found.

PROBABLE CAUSE

27. Based on my training, experience, and the information contained in this affidavit, there is probable cause to believe that the **Target Domain** is subject to both civil and criminal forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1), as property involved in money laundering.

28. Laurene Mitchel (“Mitchel”) is the name associated with social media accounts involved in the perpetration of a so-called “pig butchering” scam. A pig butchering scam typically

involves individuals (who are often located overseas) who adopt fake online identities in an effort to gain a victim's affection and trust. Once a level of trust is developed by the victim, the fraudsters use the close relationship to manipulate the victims into sending the fraudsters money, often via wire transfer. The funds are reported to be in fake cryptocurrency investment accounts. The term "pig butchering" arises from an analogy comparing the initial phase of gaining the victims' trust to the fattening of pigs before slaughtering them.

29. The Victim is a middle-aged man who resides in Warren County, New York. The Victim has a Facebook account and uses it to communicate with other Facebook users.

30. Beginning around June 2023, the Victim began receiving messages from an individual purporting to be Mitchel on Facebook messenger. According to the Victim, Mitchel used a Facebook account in the name of "Laurene Mitchel." After meeting on Facebook, the Victim and Mitchel communicated on WhatsApp. Mitchel encouraged the Victim multiple times to "invest" in cryptocurrency using the platform NFT-UNI.com, the **Target Domain**.

31. Investigation revealed the **Target Domain** is not a legitimate cryptocurrency platform and is instead a domain controlled by fraudsters used to mimic a legitimate cryptocurrency platform. That is based on the following investigative findings:

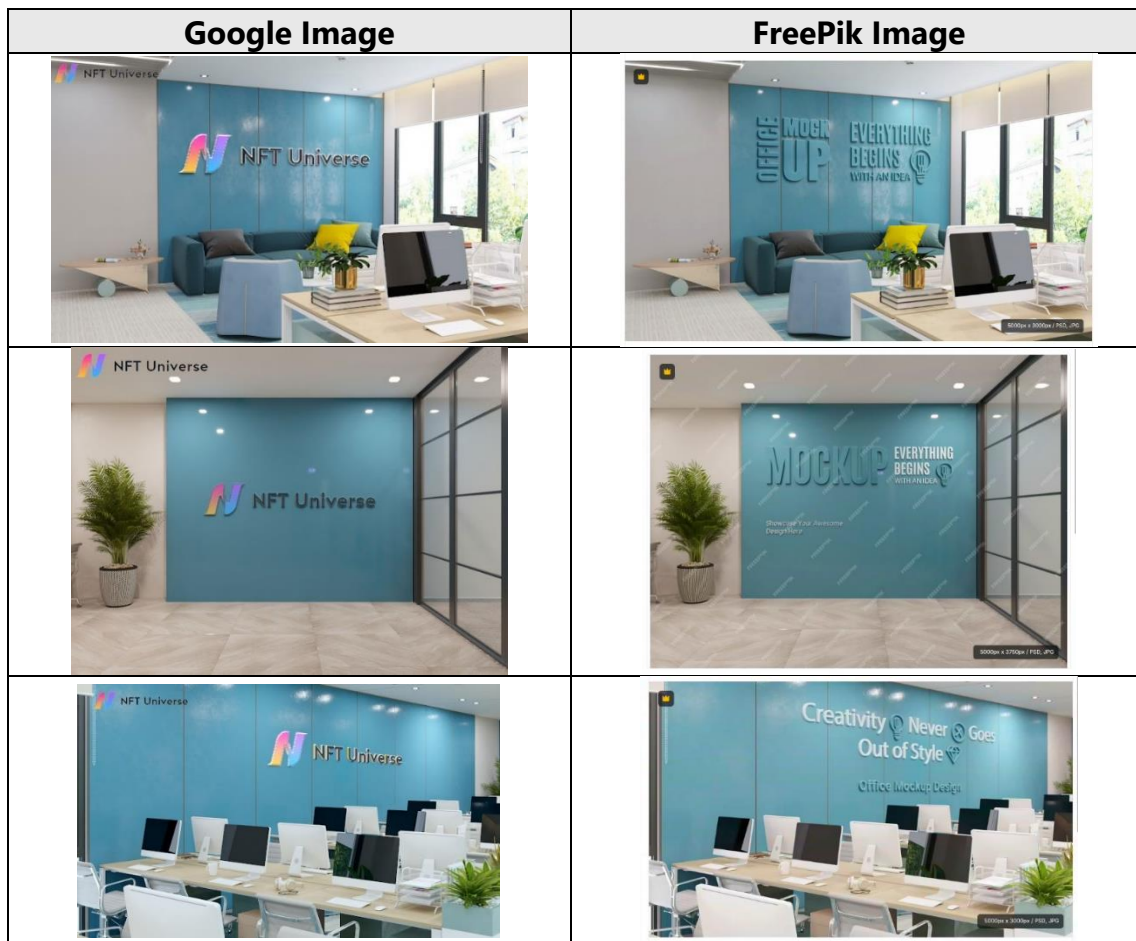
- a. The illegitimate domain NFT-UNI.com uses a logo that can be described as an "N", which transitions in color from yellow, to pink, to blue, and to purple. A copy is below:

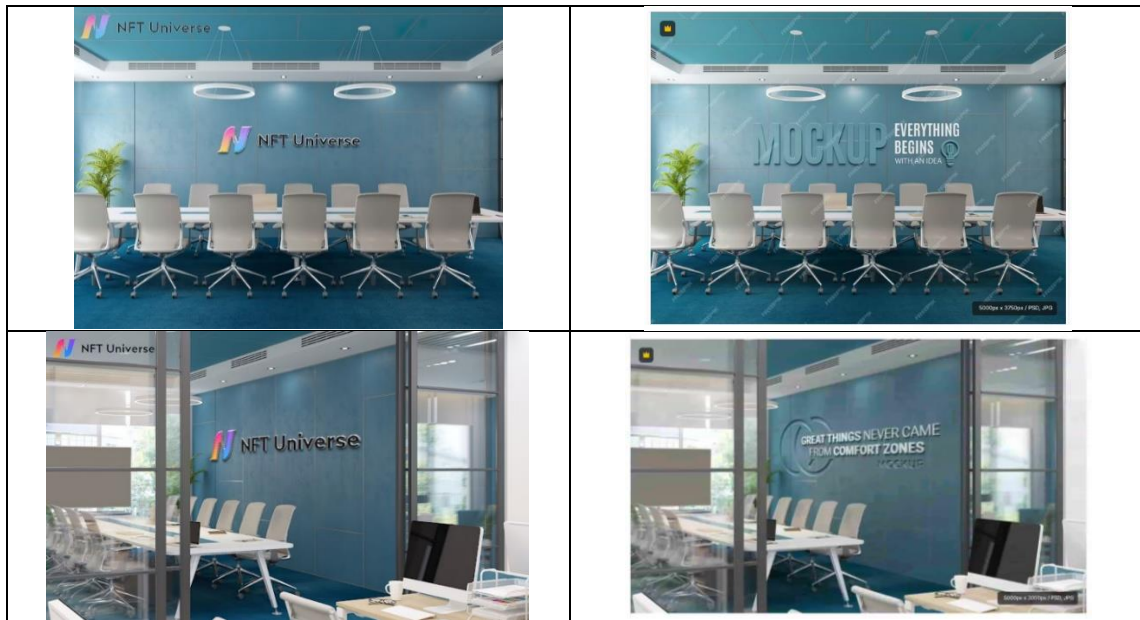


- b. On March 12, 2025, analysts with the Secret Service performed a Google search for "NFT Universe" and located a Google business entry for "NFT-Universe"

here: <https://g.co/kgs/3iLJE2Q>. The entity used a matching logo to the identified website and had an associate website of <https://nft-uni.com/>.

- c. The listed address was 15b, 1 Angel Ct, City of London, London EC2R 7HJ, United Kingdom and the listed phone number was +44 7415 954247. A search of the business registry in the United Kingdom indicated there was no registered business called NFT Universe, and nothing similarly named.
- d. In addition, the listing had six unique images uploaded by the user “NFT- Universe” which appeared to be office spaces with the NFT Universe company logo. Open-source research located similar versions of five of the pictures on image customization site FreePik. A side-by-side comparison is below:





- e. Open-source research located a registered entity in Colorado called NFT-UNIVERSE INC, assigned Secretary of State identification number 20238173362, which was formed in 2023. As of May 12, 2025, that entity was in a non-compliant status for failing to file a periodic report as of February 1, 2025, and was scheduled to become delinquent on March 31, 2025.
- f. Secret Service analysts located two additional websites which substantially matched the overall structure, company names, and company logo of “NFT-UNI.com”. Investigators recognize these websites to be duplicate websites, which are exact or substantially similar copies of websites at different URL addresses. Criminal organizations often use duplicate sites to keep versions of illicit sites open after websites are taken down. The other URL addresses were “opensea-auction.com” and “nft-uniapp.com”.
- g. In addition, the domain name records for all three sites indicated they were associated to CloudFlare. CloudFlare is a third-party service which masks domain name service records (the routing of domain names to the website

hosting server). All three domain names also had active leases. The service can be used by legitimate users attempting to mask their personal information for a website registration. Based on my training and experience, I know that the use of CloudFlare is a common obfuscation technique used by crypto fraud perpetrators.

- h. Information obtained from CloudFlare indicated that all three websites were hosted by Amazon Web Services servers in Singapore. Based on my training and experience, a U.S. or European based entity would not typically host its website in a Singapore based server.
- i. Furthermore, a search on complaints on the FBI Internet Crime Complaint Center revealed that “NFT-UNI.com” was listed in 18 victim complaints. The loss associated with these 18 victims approximated \$4,564,936.47 of adjusted loss.

32. Between November of 2023 and March 2024, the Victim, at the suggestion and direction of Mitchel, sent multiple cryptocurrency transfers that were intended to be investments in cryptocurrency. The Victim cumulatively wired approximately \$170,000.00 to crypto wallets used by the suspects involved in the scheme after receiving specific instructions from individuals purporting to be Customer Support for NFT-UNI.com via the domain NFT-UNI.com.

33. On May 28, 2024, the Secret Service interviewed the Victim. The Victim told agents the following:

- a. He had initially met Mitchel on Facebook and was encouraged by her to start investing in cryptocurrency.
- b. The Victim was encouraged and coached by Mitchel to create an account using

NFT-UNI.com, where the Victim would supposedly invest in cryptocurrency.

The Victim sent multiple cryptocurrency transfers to cryptocurrency wallets that he thought were owned and operated by NFT-UNI.com.

- c. The Victim had chats with individuals from “customer service” on the domain NFT-UNI.com; these contacts provided the Victim with wiring instructions, containing the crypto wallet address: 0x1111111254eeb25477b68fb85ed929f73a960582 (“Crypto Wallet 60582”).
- d. When the Victim tried to withdraw funds, he was told by NFT-UNI.com “customer service” that he would have to make additional payments that were required for “taxes” or “fees” to withdraw any money.

34. Cryptocurrency tracing was conducted, and the following cryptocurrency transactions were sent from the Victim’s crypto wallet, to the NFT-UNI.com wallet:

- a. On November 29, 2023, the Victim sent 3.50533943 Ethereum, worth \$13,196.69 to the Crypto Wallet 60582.
- b. On December 14, 2023, the Victim sent 2.22273694 Ethereum, worth \$8,368.00 to the Crypto Wallet 60582
- c. On January 17, 2024, the Victim sent 3.90499259 Ethereum, worth \$14,701.28 to the Crypto Wallet 60582
- d. On February 5, 2024, the Victim sent 4.07833164 Ethereum, worth \$15,353.86 to the Crypto Wallet 60582.
- e. On February 26, 2024, the Victim sent 16.98327305 Ethereum, worth \$63,937.71 to the Crypto Wallet 60582.
- f. On February 26, the Victim sent 0.61411067 Ethereum, worth

\$2,311.97 to the Crypto Wallet 60582.

- g. On March 27, 2024, the Victim sent 14.48602000 Ethereum, worth \$54,536.10 to the Crypto Wallet 60582.

35. The Victim requested to withdraw funds from the “account” multiple times but was told additional payments for “taxes” or “fees” were required in order make withdrawals. The Victim was able to provide screenshots of messages communicating with NFT-UNI.com, “online customer service,” some of the communications are described below:

- a. The Victim received the following message on the domain NFT-UNI.com, “Hello, you currently need to upgrade your membership level to make withdrawals. To upgrade your membership level, you need to accumulate an actual deposit of 200,00 USDT to upgrade your membership level.”
- b. The Victim received the following message on the domain NFT-UNI.com, “Hello, if you have not upgraded to a premium membership before March 27, your account will be permanently frozen. This is due to system rules and cannot be controlled by humans.”
- c. The Victim received the following message on the domain NFT-UNI.com, “Hello, the reason why you cannot withdraw money has been found. The system shows that your account is a multi-account recharge, so the system thinks that you are suspected of money laundering activities.”
- d. The Victim received the following message on the domain NFT-UNI.com, “Hello, in order to ensure the safety of your funds, you must a pay a 30% deposit before April 30 to ensure the safety of your funds.”
- e. The Victim received the following message on the domain NFT-UNI.com,

“Hello, if you do not pay your 30% deposit by April 30th, you will be required to pay more when it is due.”

- f. The Victim received the following message on the domain NFT-UNI.com, “Hello, because your account is suspected of multi-account recharge, suspected of money laundering activities, NFT account belongs to the personal account, does not belong to the multi-accounts.”
- g. The Victim received the following message on the domain NFT-UNI.com, “Hello, due to the fact that your account is suspected of being funded by more than one account, you are currently required to make a 30% deposit to keep your account up and running. If you do not complete this 30% deposit, your account will be frozen!”

USSS Investigation Reveals Money Laundering of Fraud Proceeds

36. The USSS’s investigation ultimately revealed that the **Target Domain** was involved in money laundering through cryptocurrency transactions. The Victim was instructed to conduct cryptocurrency transactions to cryptocurrency wallets, with the individuals engaged in fraud using the **Target Domain** receiving the cryptocurrency funds.

37. Based on public sources and my training and experience, I understand the following:

- a. 1inch Network is a decentralized finance (“DeFi”) platform and liquidity aggregator that is designed to scrap through a handful of decentralized cryptocurrency exchanges in search of the best market price for a given cryptocurrency on cryptocurrency platforms.¹

¹ For more information on 1inch, see <https://1inch.io/> (last visited March 30, 2025) (“One-stop access to decentralized finance.”).

- b. “Wrapped Ethereum” is an ERC-20 token that represents the cryptocurrency Ethereum and is pegged 1:1 to the value of Ethereum. Wrapped Ethereum can be used to interact with other DeFi protocols and applications whereas Ethereum, the cryptocurrency, by itself, cannot be used in many decentralized applications (“dApps”).
- c. “ERC-20” is a standard for fungible tokens on the Ethereum blockchain. Short for “Ethereum Request for Comments 20,” ERC20 defines a set of rules and functions that Ethereum-based tokens must adhere to, ensuring interoperability and compatibility with the various applications, wallets, crypto exchanges, and smart contracts across the Ethereum ecosystem.²
- d. A decentralized application or “dApp” is a type of open-source software program that runs on a distributed peer-to-peer (P2P) network, such as a blockchain.³
- e. A stablecoin is a digital asset that remains stable in value against a pegged external traditional asset class. For example, Tether (known by its symbol USDT) is pegged to the U.S. dollar and remains stable over time.

38. Once the deposits were made into Crypto Wallet 60582, the cryptocurrency was subsequently transferred out of the wallet into and made inaccessible to the Victim. The funds were transferred from the victim’s wallet to a wallet associated with 1inch Network. Based on public sources and my training and experience,

39. Cryptocurrency tracing has further found that the funds were then transferred from

² For more information on ERC-20, see <https://www.moonpay.com/learn/cryptocurrency/what-is-erc20> (last visited March 30, 2025).

³ For information on dApps, see <https://www.moonpay.com/learn/defi/what-are-dapps> (last visited March 30, 2025).

the 1inch Network wallet into a Wrapped Ethereum contract.

40. Once in the wrapped Ethereum contract, the funds were sent back to the 1inch Network. Once in the 1inch Network, the funds were converted to Tether. All of the victims funds were sent to the same wallet with address 0xc9c0c3af7c6e0aabfe88818352e59e80976ca981.

41. Based on my training and experience, the rapid transfers of cryptocurrency between different wallets, such as the sequence of events described above, is a common method used by those involved in money laundering activities. Otherwise, the funds would go directly from the 1-inch-network directly to the intended wallet, without the need to send the funds to a wrapped Ethereum contract, then swap it for USDT/Tether, because it incurs many more fees that would not be financially prudent. The multiple layers of transfers, wraps, and swaps, indicate an intent to conceal the source and destination of the funds. Those actions incurred additional fees which any prudent investor would likely want to avoid spending, unless furthering dispersion of funds to make it harder to trace.

42. Based on my training and experience, I know that criminally derived funds are often laundered cryptocurrency transactions before ultimately returning to a criminal actor or actors, near or at the top of a criminal organization's hierarchy.

The Target Domain

43. As described above, the **Target Domain**, NFT-UNI.com, was used to perpetrate a pig butchering scam, and was the platform through which the persons engaged in fraud laundered the Victim's money.

44. A search of publicly available WHOIS domain name registration records revealed that the **Target Domain** was registered on or about November 3, 2023, through the registrar Gname.com Pte. Ltd., which has its headquarters in Singapore. The publicly available WHOIS

database lists the registrant of the **Target Domain** as “Redacted for privacy” in Hong Kong and the name server as CloudFlare.

45. The top-level domain for the **Target Domain** is Verisign. Verisign currently manages all “.com” domains.

46. I last visited the **Target Domain** on March 20, 2025, which showed that the site remains active.

CONCLUSION AND REQUEST FOR RELIEF

47. Based on the foregoing, there is probable cause to believe that the **Target Domain** is property involved in pig-butcher (crypto-currency) offenses in violation of 18 U.S.C. § 1956 (a)(1)(B)(i), and is thereby subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and to criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

48. Authority is sought to seize the **Target Domain** pursuant to 21 U.S.C. § 853(f). By seizing the **Target Domain** and redirecting it to another website, the government will prevent continued use of the **Target Domain** to commit additional crimes. Furthermore, seizure of the **Target Domain** will prevent third parties from continuing to access the **Target Domain’s** websites in their present form. Accordingly, restraint pursuant to 21 U.S.C. § 853(e) would be insufficient.

49. Therefore, I respectfully request that a seizure warrant be issued for the **Target Domain** pursuant to 18 U.S.C. § 981(b)(1), and 21 U.S.C. § 853(f) by 18 U.S.C. § 982(b)(1), for forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1).

SEIZURE PROCEDURE

50. As detailed in Attachment A, upon execution of the seizure warrant, VeriSign, Inc., for the **Target Domain**, headquartered at 12061 Bluemont Way in Reston, VA, shall be directed

to restrain and lock the **Target Domain** pending transfer of all right, title, and interest in the **Target Domain** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **Target Domain** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the Secret Service or Department of Justice.

51. In addition, upon seizure of the **Target Domain** by the Secret Service, VeriSign, Inc. will be directed to associate the **Target Domain** to a new authoritative name server(s) to be designated by a law enforcement agent. The government will display a notice on the website to which the Target Domain will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

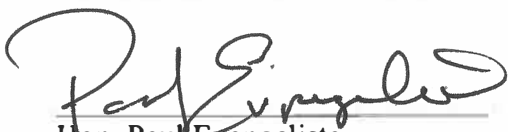
52. Because the warrant will be served on VeriSign, Inc., which controls the Target Domain, and VeriSign, Inc. thereafter, at a time convenient to it, will transfer control of the Target Domain to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Attested to by the affiant,



William Thompson Henry
Special Agent
United States Secret Service

I, the Hon. Paul Evangelista, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on April 4th, 2025, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure:



Hon. Paul Evangelista
United States Magistrate Judge

ATTACHMENT A

With respect to **NFT-UNI.com** (“**NFT-UNI**”), VeriSign, Inc. (“VeriSign”), who is the top-level domain registry for the **NFT-UNI**, shall take the following actions to effectuate the seizure of **NFT-UNI**:

- 1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the United States Secret Service, by modifying the **NFT-UNI** authoritative DNS server entries to include the following:

(a) ns1.usssdomainseizure.com

(b) ns2.usssdomainseizure.com

or:

Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to VeriSign, Inc.

- 2) Prevent any further modification to, or transfer of, **NFT-UNI** pending transfer of all right, title, and interest in **NFT-UNI** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **NFT-UNI** cannot be made absent court order or, if forfeited to the United States, without prior consultation with United States Secret Service.
- 3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
- 4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

- 5) The Government will display a notice on the website to which the **NFT-UNI** will resolve.

That notice will consist of law enforcement emblems and the following text (or substantially similar text):

THIS DOMAIN HAS BEEN SEIZED

This domain has been seized pursuant to a seizure warrant issued by the United States District Court for the Northern District of New York in accordance with 18 U.S.C. §§ 981 and 982 and 21 U.S.C. § 853(f), as part of a law enforcement action by:

U.S. Department of Justice – Northern District of New York

U.S. Secret Service – Empire State Cyber Fraud Task Force

If you are a victim of this alleged fraud, please visit

<https://www.secretservice.gov/contact/field-offices> and contact your local Field Office for more information and victim reporting.